JOURNAL OF ALGEBRA 144, 399–410 (1991)

Group Structure Computations in Finite Chain Rings

M. A. DE LUIS

Arlamendi, 6-4°-B, Las Arenas, 48930 Getxo, Vizcaya, Spain

Communicated by Walter Feit

Received December 19, 1989

INTRODUCTION

Interest in the structure of the unit group R^* of a finite ring R goes a long way back. In 1910 Ranum [10] obtained the structure of the unit group of every residue ring of the ring of integers of a quadratic number field. Recently, Cross [4], apparently unaware of Ranum's work, determined the structure of the group of units of the residue rings of the Gaussian integers. The invariants of $(K[x]/(f))^*$ (K a finite field, f a polynomial) were obtained by Claasen in [3]. His work was later simplified by Smits in [12]. Raghavendran in [9] obtained the structure of R^*, when R is a Galois ring, i.e., a finite commutative chain ring whose maximal ideal is pR (p prime). Galois rings are important in structural issues concerning finite rings; see [7, Chap. XIX, p. 368]. There has been interest too in the structure of R_+ (the additive group of the ring R); e.g., Clark and Drake determined the additive structure of a finite chain ring [5, Corollary to Theorem 1].

The methods used by the authors cited above give no idea as to how to proceed in situations other than those they discuss. The aim of this paper is to show that a rather elementary fact about finite abelian p-groups (i.e., that the structure of such groups is determined by the number of elements of each order in the group) provides a general-purpose computational tool for handling the type of problems mentioned above. After presenting this fact in Section 1 (Proposition 1), we make three applications.

Firstly (in Section 2), we determine the additive structure of the powers M^s of the maximal ideal M of a finite chain ring R. When R is, in addition, commutative, the structure of $(M^s)_+$ (i.e., M^s as an additive group) follows from Ayoub [2, Theorem 2, p. 387], a result that uses the theory of j-diagrams developed in [1].

Next (in Section 3), we apply Proposition 1 to give a new derivation of the structure of R^*, when R is a Galois ring (cf. [9, Theorem 9, p., 215]).

0021-8693/91 $3.00

Finally (in Section 4), we give a straightforward derivation of the structure of the group of units of a finite commutative chain ring, with prime characteristic. We note that any such ring R is determined, up to isomorphism, by three independent parameters, p, d, e, where $p = \text{char } R$, $p^d = |K|$ (K the residue field of R), and e is the nilpotency index of the maximal ideal of R [6, Lemma 1]. Our Theorem 3 gives a simple algorithm to compute the structure of R^*, taking as input the said parameters. When R is represented as $K[x]/(x^e)$, K a finite field [6, Lemma 1], this algorithm is to be viewed as an alternative to that implicit in [12].

0. Preliminaries

Our rings are finite and have $1 \neq 0$. The group of units of a ring R is written as R^*. A ring R is *local* iff the set of non-units is closed under addition. This set is an ideal which contains any proper ($\neq R$) left (right) ideal of R. It is called the *maximal* ideal of R; we denote it by M. As it is immediate that $M = J(R)$, the Jacobson radical of R, it follows that M is nilpotent [7, Theorem 4.7, p. 75]. For a local ring R with maximal ideal M, R/M is a finite field, called the *residue field* of R. We denote it by K. In a finite ring R "the lattice of left ideals is a chain" is equivalent to "the lattice of right ideals is a chain" (see [5, Lemma 1]). When a ring satisfies either of these conditions it is said to be a *chain ring*; such a ring is clearly local. In a chain ring R, all ideals are two-sided and both left and right principal; i.e., R is a principal ideal ring [5, Lemma 1]. Furthermore, the following "size" formulae hold: $|M^i| = |K|^{e-i}$ $(0 \leqslant i \leqslant e)$, where e is the nilpotency index of M [8, Lemma 1.2]. As, in particular, $|R| = |M^0| = |K|^e$, it follows that R is a p-ring. So if $\text{char } R \neq p$, then $p1_R \in M^r \setminus M^{r+1}$ $(1 \leqslant r \leqslant e-1)$. We call this parameter r the *ramification index* of R.

Let G be a finite abelian group. If $E \subseteq G$ satisfies that all its elements have the same order, we say that E is *order-homogeneous* and write $o(E)$ for the common order of the elements in E. The rank of G (i.e., the smallest number of generators for G) is written $\text{rk}(G)$. A cyclic group of order n is denoted by C_n. If G is a finite abelian p-group, we write its structure as $G \cong l_1 C_p \otimes l_2 C_{p^2} \otimes \cdots \otimes l_j C_{p^j} \otimes \cdots$, where l_j is the number of copies of C_{p^j} (clearly $l_j = 0$, for large j). Finally, if x is a rational number, then $\text{int}_+(x)$ denotes $\min\{n \in \mathbb{Z} \mid x \leqslant n\}$.

1. An Algorithm to Compute Group Structure

In this section we present our basic tool for the structure computations we undertake in the subsequent sections. It is stated in Sandling [11, Lemma 1.1]; we give the proof for completeness.

PROPOSITION 1. *Let G be a finite abelian p-group and (l_j) a sequence of integers $(l_j \geqslant 0)$ such that $G \cong l_1 C_p \otimes l_2 C_{p^2} \otimes \cdots \otimes l_j C_{p^j} \otimes \cdots$. Define the sequences (N_j) and (k_j) by the following identities:*

$$N_j = |\{g \in G \mid o(g) \leqslant p^j\}|, \qquad \text{and} \qquad k_j = \log_p(|G|/N_j) \qquad (j = 0, 1, 2, \ldots).$$

Then

$$l_j = k_{j-1} - 2k_j + k_{j+1} \qquad (j = 1, 2, \ldots).$$

Proof. Put $G_j = G^{p^j}$ $(j = 0, 1, \ldots)$. For each j, $\theta_j: G \to G_j$ $(\theta_j(g) = g^{p^j}, \forall g \in G)$ and $\lambda_j: G_j \to G_{j+1}$ $(\lambda_j(g) = g^p, \forall g \in G_j)$ are epimorphisms. Hence $|G|/|\ker \theta_j| = |G_j|$ and $|G_j|/|G_{j+1}| = |\ker \lambda_j|$ $(j = 0, 1, \ldots)$. If we note that $|\ker \theta_j| = N_j$ and that $|\operatorname{Ker} \lambda_j| = |\{g \in G_j \mid g^p = 1\}| = p^{\operatorname{rk}(G_j)}$, it follows that

$$\begin{aligned} \operatorname{rk}(G_j) &= \log_p(|G_j|) - \log_p(|G_{j+1}|) = \log_p(|G|/N_j) - \log_p(|G|/N_{j+1}) \\ &= k_j - k_{j+1} \qquad (j = 0, 1, \ldots). \end{aligned} \tag{1}$$

By powering G to p^{j-1} and p^j, respectively, we obtain

$$\begin{aligned} G_{j-1} &\cong l_1 C_1 \otimes \cdots \otimes l_{j-1} C_1 \otimes l_j C_p \otimes l_{j+1} C_{p^2} \otimes \cdots \\ G_j &\cong l_1 C_1 \otimes \cdots \otimes l_{j-1} C_1 \otimes l_j C_1 \otimes l_{j+1} C_p \otimes \cdots. \end{aligned}$$

If we take ranks,

$$\operatorname{rk}(G_{j-1}) = l_j + l_{j+1} + \cdots; \qquad \operatorname{rk}(G_j) = l_{j+1} + l_{j+2} + \cdots.$$

Hence

$$l_j = \operatorname{rk}(G_{j-1}) - \operatorname{rk}(G_j) \qquad (j = 1, 2, \ldots).$$

Therefore by (1), $l_j = (k_{j-1} - k_j) - (k_j - k_{j+1}) = k_{j-1} - 2k_j + k_{j+1}$, as required. ∎

In the following sections, we apply this result by first obtaining explicit formulae to compute the order of any element in the group whose structure we seek. This leads to a natural way of breaking up the group as a pairwise disjoint union of order-homogeneous classes. Then, we obtain formulae to compute the N_j of the group. Once this has been accomplished, the k_j are computed by $k_j = \log_p(|G|/N_j)$ and finally the structure is "read off" by means of $l_j = k_{j-1} - 2k_j + k_{j+1}$.

2. ADDITIVE GROUPS IN CHAIN RINGS

Let R be a finite chain ring, with maximal ideal M. Our first application of Proposition 1 is to compute the structure of M^s, viewed as a group under addition (Theorem 1). By convention, we take $M^0 = R$.

The next proposition is in preparation for the proof of the following theorem; it gives the necessary order information for applying Proposition 1.

PROPOSITION 2. *Let e be the nilpotency index of the maximal ideal M of a finite chain ring R. Assume that* char $R \neq p$ ($p^d = |R/M|$), *and let r be the ramification index of R. If $x \in M^t \setminus M^{t+1}$ $(0 \leqslant t \leqslant e-1)$, then*

$$o_+(x) = p^{\operatorname{int}_+((e-t)/r)}$$

(where $o_+(x)$ denotes the additive order of x).

Proof. Since R is a chain ring, $|R| = |K|^e = p^{de}$ ($K = R/M$, i.e., the residue field of R). Thus $o_+(x)$ is a p-power for any $x \in R$. Therefore

$$o_+(x) = p^n, \qquad \text{with} \quad n = \min\{1 \leqslant i \mid p^i x = 0_R\}. \tag{1}$$

Let π be a generator for M. Observing that $\pi^t R = R\pi^t = M^t$ [5, Lemma 1], $x \in M^t \setminus M^{t+1} \Leftrightarrow x = \alpha\pi^t$ ($\alpha \in R^*$). Similarly, by the definition of the ramification index, $p = \varepsilon\pi^r$ ($\varepsilon \in R^*$). By induction, $p^i = \mu_i \pi^{ri}$ ($\mu_i \in R^*$). Hence $p^i x = 0_R \Leftrightarrow \mu_i \pi^{ri} \alpha \pi^t = 0_R$. Now $\mu_i(\pi^{ri}\alpha)\,\pi^t = \mu_i(\beta\pi^{ri})\,\pi^t = \mu_i \beta \pi^{ri+t}$, for some $\beta \in R^*$ (note that as $\pi^{ri}\alpha = \beta\pi^{ri}$, for some $\beta \in R$, and $\alpha \in R^*$, we ought to have $\beta \in R^*$; else $\beta\pi^{ri} \in M^s$ with $s > ri$, yet $\beta\pi^{ri} = \pi^{ri}\alpha \in M^{ri} \setminus M^{ri+1}$). It follows that $p^i x = 0_R \Leftrightarrow \mu_i \beta \pi^{ri+t} = 0_R \Leftrightarrow \pi^{ri+t} = 0_R$ (because both μ_i, β are units). The last identity is equivalent to $e \leqslant ri + t$; hence (see definition of n above)

$$\begin{aligned} n &= \min\{1 \leqslant i \mid p^i x = 0_R\} = \min\{1 \leqslant i \mid e \leqslant ri + t\} \\ &= \min\{1 \leqslant i \mid (e-t)/r \leqslant i\} = \operatorname{int}_+((e-t)/r). \end{aligned}$$

Substituting this into (1) yields the required result. ∎

THEOREM 1. *Let M be the maximal ideal of a finite chain ring R, e the nilpotency index of M, and $|R/M| = p^d$ (p prime). Say $(M^s)_+$ denotes M^s viewed as a group under addition $(0 \leqslant s \leqslant e-1)$.*

(a) *If* char $R = p$, *then*

$$(M^s)_+ \cong C_p \otimes \cdots^{d(e-s)} \otimes C_p.$$

(b) *If* char $R \neq p$ *and r is the ramification index of R, then*

$$(M^s)_+ \cong C_{p^m} \otimes \cdots^{d(r-v)} \otimes C_{p^m} \otimes C_{p^{m+1}} \otimes \cdots^{dv} \otimes C_{p^{m+1}}$$

(where $e - s = mr + v$, $0 \leqslant v < r$).

Proof. (a) is clear; note that $|M^s| = |K|^{e-s} = p^{d(e-s)}$, and as char $R = p$, $(M^s)_+$ has to be elementary abelian. As for (b), we apply Proposition 1. To this end, we need the N_j of $(M^s)_+$. Recalling the definition of N_j (Proposition 1), we see that

$$N_0 = 1 \qquad \text{and} \qquad N_j = |K|^{e-s}, \qquad \text{for} \quad j \geqslant \operatorname{int}_+((e-s)/r). \tag{1}$$

The first of these is clear. The others follow from $|M^s| = |K|^{e-s}$ and the fact that, by Proposition 2, the largest order for the elements in M^s is p^n with $n = \operatorname{int}_+((e-s)/r)$.

To compute N_j, for $1 \leqslant j < \operatorname{int}_+((e-s)/r)$, we break up M^s:

$$M^s = \{0_R\} \cup \bigcup_{t=s}^{e-1} S_t, \qquad \text{with} \quad S_t = M^t \backslash M^{t+1}. \tag{2}$$

By Proposition 2 the classes S_t are order-homogeneous and $o(S_t) = p^n$, with $n = \operatorname{int}_+((e-t)/r)$. Evidently $o(S_t)$ decreases as t increases. Thus by the definition of N_j (Proposition 1) and (2),

$$\begin{aligned} N_j &= |\{\gamma \in M^s \mid o(\gamma) \leqslant p^j\}| \\ &= 1 + \sum_{t=t(j)}^{e-1} |S_t|, \qquad \text{with} \quad t(j) = \min\{t \geqslant s \mid o(S_t) \leqslant p^j\}. \end{aligned} \tag{3}$$

As $|S_t| = |M^t| - |M^{t+1}| = |K|^{e-t} - |K|^{e-t-1}$, it follows that

$$N_j = 1 + \sum_{t=t(j)}^{e-1} (|K|^{e-t} - |K|^{e-t-1}) = |K|^{e-t(j)}, \qquad 1 \leqslant j < \operatorname{int}_+((e-s)/r). \tag{4}$$

To compute $t(j)$, observe that by Proposition 2

$$o(S_t) \leqslant p^j \Leftrightarrow p^{\operatorname{int}_+((e-t)/r)} \leqslant p^j.$$

But $\operatorname{int}_+((e-t)/r) \leqslant j \Leftrightarrow (e-t)/r \leqslant j \Leftrightarrow e - rj \leqslant t$. Hence $o(S_t) \leqslant p^j \Leftrightarrow e - rj \leqslant t$. Now $j < \operatorname{int}_+((e-s)/r) \Leftrightarrow j < (e-s)/r \Leftrightarrow s < e - rj$. Thus $t(j) = e - rj$ (definition of $t(j)$ in (3)) and by (4), $N_j = |K|^{rj}$, $1 \leqslant j < \operatorname{int}_+((e-s)/r)$. As the other N_j's are known from (1), we have

$$N_j = |K|^{rj}, \ 0 \leqslant j < \operatorname{int}_+((e-s)/r); \qquad N_j = |K|^{e-s}, \ j \geqslant \operatorname{int}_+((e-s)/r).$$

The definition of k_j (Proposition 1) and the fact that $|M^s| = |K|^{e-s}$ give

$$k_j = d(e - rj - s), \ 0 \leqslant j < \operatorname{int}_+((e-s)/r); \qquad k_j = 0, \ j \geqslant \operatorname{int}_+((e-s)/r). \tag{5}$$

If we now let $e - s = mr + v$ $(0 \leqslant v < r)$, we see that

$$\operatorname{int}_+((e-s)/r) = m + \operatorname{int}_+(v/r) = \begin{cases} m & \text{if} \quad v = 0; \\ m+1 & \text{if} \quad v \neq 0. \end{cases} \tag{6}$$

So when $v \neq 0$, (5) yields

$$k_j = d(e - rj - s),\ 0 \leqslant j \leqslant m; \qquad k_j = 0,\ j > m. \tag{7}$$

When $v = 0$, we see from (5) and (6) that (7) still holds. Then, from (7), using the identity $l_j = k_{j-1} - 2k_j + k_{j+1}$ of Proposition 1, an easy calculation gives

$$l_j = 0,\ 1 \leqslant j \leqslant m-1; \qquad l_m = d(r - v); \qquad l_{m+1} = dv; \qquad l_j = 0,\ j \geqslant m+2.$$

Thus $(M^s)_+$ has the required structure. ∎

COROLLARY (cf. [2, p. 388]). *For the setting in Theorem* 1:

(a) *If* char $R = p$, *then*

$$M_+ \cong C_p \otimes \cdots^{d(e-1)} \otimes C_p;$$

in particular $\mathrm{rk}(M_+) = d(e-1)$.

(b) *If* char $R = p^n$ $(n > 1)$, *and* r *is the ramification index of* R, *then*

$$M_+ \cong C_{p^{n-1}} \otimes \cdots^{d(r-v)} \otimes C_{p^{n-1}} \otimes C_{p^n} \otimes \cdots^{dv} \otimes C_{p^n}$$

(*where* $e - 1 = mr + v$, $0 \leqslant v < r$); *in particular* $\mathrm{rk}(M_+) = dr$.

Proof. (a) is obvious from Theorem 1(a). For (b), note that char $R = o_+(1_R)$. Hence by Proposition 2 with $t = 0$, $n = \mathrm{int}_+(e/r)$. Now in Theorem 1(b) with $s = 1$, $e - 1 = mr + v$. Hence $\mathrm{int}_+(e/r) = \mathrm{int}_+((mr + v + 1)/r) = m + \mathrm{int}_+((v+1)/r)$. But $0 \leqslant v < r$, and thus $0 < (v+1)/r \leqslant 1$. Then $\mathrm{int}_+((v+1)/r) = 1$. Therefore $n = m + 1$, and thus Theorem 1(b), with $s = 1$, yields the structure assertion in (b) of the corollary. The rank assertion is then clear. ∎

Note. For the convenience of the reader, we state a result which is used in the following sections. *If* R *is a finite commutative local ring with maximal ideal* M *and residue field* K $(K = R/M)$, *then* $R^* = (1 + M) \otimes H$, *where* H *is a subgroup of* R^* *isomorphic to* K^* [7, Theorem 18.2, p. 355].

3. The Group of Units of a Galois Ring

Galois rings can be defined in various equivalent ways, but however they are defined, it is well known that R is a Galois ring iff R is a finite commutative chain ring with maximal ideal $M = pR$, p a prime [7, p. 308].

In order to apply Proposition 1, we need , first, order information on the elements of the one-group $1 + M$ of the Galois ring R.

PROPOSITION 3. *Let R be a Galois ring with maximal ideal $M = pR$ (p prime). Assume that $e \geqslant 2$, where e is the nilpotency index of M. Let $G_0 = 1 + M$, viewed as a group under multiplication. Then we have the following pairwise disjoint decomposition of G_0:*

$$G_0 = \{1_R\} \cup \bigcup_{t=1}^{e-1} 1_R + M^t \backslash M^{t+1}.$$

Moreover, let $\gamma \in 1_R + M^t \backslash M^{t+1}$ $(1 \leqslant t \leqslant e-1)$.

(a) *If p is odd or if $p = 2$, but $2 \leqslant t \leqslant e-1$, then $o(\gamma) = p^{e-t}$.*

(b) *If $p = 2$ and $\gamma \in 1 + M \backslash M^2$, then $\gamma = -1_R$ or $\gamma \in -1_R + M^s \backslash M^{s+1}$ $(1 \leqslant s \leqslant e-1)$ and in the latter case $o(\gamma) = 2^{e-s}$.*

Proof. The first assertion is clear, since $M = \{0_R\} \cup \bigcup_{t=1}^{e-1} M^t \backslash M^{t+1}$ and $G_0 = 1 + M$. For (a), note that as $p1_R$ (henceforth written as p) is a generator for M, $\gamma \in 1 + M^t \backslash M^{t+1} \Leftrightarrow \gamma = 1 + p^t\alpha$ $(\alpha \in R^*)$. To obtain $o(\gamma)$, note that $|1 + M| = |M| = |K|^{e-1}$ (i.e., a p-power); hence we need to look at the p-powers of γ.

By expanding $(1 + p^t\alpha)^p$ and observing that $p \mid \binom{p}{i}$ $(1 \leqslant i \leqslant p-1)$ and that as for the term $(p^t\alpha)^p$, $1 + t < pt$ $(\Leftrightarrow 1 < (p-1)t)$ always holds under the assumptions in (a), we obtain $\gamma^p = 1 + p^{t+1}\alpha_1$, for some $\alpha_1 \in R^*$. As this has the same form as the expression for γ, after this powering process is iterated i times, it follows that

$$\gamma^{p^i} = 1 + p^{t+i}\alpha_i \qquad (\alpha_i \in R^*).$$

Therefore

$$\gamma^{p^i} = 1 \Leftrightarrow p^{t+i} = 0 \Leftrightarrow e \leqslant t + i \Leftrightarrow e - t \leqslant i.$$

It is then clear that $o(\gamma) = p^{e-t}$. This proves (a).

As for (b), let $\gamma \in 1 + M \backslash M^2$. Then $\gamma = 1 + 2\alpha = -1 + 2(1 + \alpha)$ $(\alpha \in R^*)$. Since $2(1 + \alpha) \in M$ and

$$M = \{0_R\} \cup \bigcup_{s=1}^{e-1} M^s \backslash M^{s+1}$$

(with the union clearly pairwise disjoint), either $\gamma = -1_R$ or there exists a unique $s \in \{1, 2, ..., e-1\}$ such that $\gamma \in -1_R + M^s \backslash M^{s+1}$. This proves the first assertion in (b).

To prove the assertion about $o(\gamma)$, let $\gamma \in -1_R + M^s \backslash M^{s+1}$ $(1 \leqslant s \leqslant e-1)$. Then $\gamma = -1 + 2^s\alpha (\alpha \in R^*)$. Hence

$$\gamma^2 = 1 - 2^{s+1}\alpha + 2^{2s}\alpha^2 = 1 + 2^{s+1}\alpha(-1 + 2^{s-1}\alpha). \tag{1}$$

We claim that $-1+2^{s-1}\alpha \in R^*$, $1 \leqslant s \leqslant e-1$. The claim is obvious, when $2 \leqslant s \leqslant e-1$. Let $s=1$; then (1) becomes $\gamma^2 = 1+2^2\alpha(-1+\alpha)$. Clearly,

$$-1+\alpha = 2^i\beta \qquad (\beta \in R^*,\ i=0, 1, ..., e). \tag{2}$$

Hence $\alpha = 1+2^i\beta$. As $\gamma = -1+2^s\alpha$ (with $s=1$), we obtain $\gamma = -1+2(1+2^i\beta) = 1+2^{i+1}\beta$. But since $\gamma \in 1+M\backslash M^2$, $i+1=1$. Therefore $i=0$, and thus by (2), $-1+\alpha = \beta \in R^*$, as claimed.

Once we have $-1+2^{s-1}\alpha \in R^*$ $(1 \leqslant s \leqslant e-1)$, we get (from (1)) that if $1 \leqslant s \leqslant e-2$, $\gamma^2 \in 1+M^{s+1}\backslash M^{s+2}$ and as then $2 \leqslant s+1 \leqslant e-1$, (a) applies with $p=2$. Hence $o(\gamma) = 2o(\gamma^2) = 22^{e-s-1} = 2^{e-s}$. If $s=e-1$, $\gamma^2 = 1$ (by (1)). As $\gamma \neq 1$, for $\gamma \in 1+M\backslash M^2$ and $M\backslash M^2 \neq 0$, it follows that $o(\gamma) = 2 = 2^{e-s}$ (with $s=e-1$). Therefore, in any event, $o(\gamma) = 2^{e-s}$. ∎

We can now give a new proof of the following result due to Raghavendran [9].

THEOREM 2. *Let R be a Galois ring, with maximal ideal $M=pR$ (p a prime) and residue field K ($|K| = p^d$).*

(a) *If p is odd, then*

$$R^* \cong C_{p^{e-1}} \otimes \cdots^{d} \otimes C_{p^{e-1}} \otimes C_{p^d-1}.$$

(b) *If $p=2$, then*

(1) $e=1 \Rightarrow R^* \cong C_{2^d-1}$;

(2) $e \geqslant 2 \Rightarrow R^* \cong C_2 \otimes C_{2^{e-2}} \otimes C_{2^{e-1}} \otimes \cdots^{d-1} \otimes C_{2^{e-1}} \otimes C_{2^d-1}$.

Proof. It is immediate that the theorem holds for $e=1, 2$. When $e=1$, $M=0$, and thus $R \cong K$; hence $R^* \cong K^* \cong C_{p^d-1}$. When $e=2$, Proposition 3 yields that G_0 is elementary abelian, and as $|G_0| = |M| = |K|^{e-1} = p^d$, it follows that $G_0 \cong C_p \otimes \cdots^{d} \otimes C_p$. Then, Theorem 18.2 of [7] (see above Note) gives $R^* \cong C_p \otimes \cdots^{d} \otimes C_p \otimes C_{p^d-1}$. Henceforth $e \geqslant 3$.

By the definition of N_j in Proposition 1 and by noting that by Proposition 3 the largest order for the elements in G_0 is p^{e-1}, we obtain

$$N_0 = 1 \qquad \text{and} \qquad N_j = |K|^{e-1}, \qquad \text{for } j \geqslant e-1. \tag{1}$$

To compute the other N_j's, let $1 \leqslant j < e-1$ and break up G_0:

$$G_0 = \{1_R\} \cup \bigcup_{t=1}^{e-1} S_t, \qquad \text{with } S_t = 1+M^t\backslash M^{t+1}. \tag{2}$$

By Proposition 3(a), classes S_t are order-homogeneous, when p is odd. When $p=2$, however, Proposition 3(b) tells us that S_1 is not order-homogeneous.

Henceforth p is odd; the case where $p=2$ is discussed later.

As $o(S_t)=p^{e-t}$ (Proposition 3(a)), we see that $o(S_t)$ decreases as t increases. Thus by (2)

$$N_j=|\{\gamma\in G_0\,|\,o(\gamma)\leqslant p^j\}|$$
$$=1+\sum_{t=t(j)}^{e-1}|S_t|,\qquad \text{with}\quad t(j)=\min\{t\geqslant 1\,|\,o(S_t)\leqslant p^j\}. \tag{3}$$

By noting that $|S_t|=|M^t|-|M^{t+1}|=|K|^{e-t}-|K|^{e-t-1}$, we obtain

$$N_j=1+\sum_{t=t(j)}^{e-1}(|K|^{e-t}-|K|^{e-t-1})=|K|^{e-t(j)},\qquad 1\leqslant j<e-1. \tag{4}$$

A simple manipulation of inequalities, using $o(S_t)=p^{e-t}$, gives $o(S_t)\leqslant p^j\Leftrightarrow e-j\leqslant t$. Then the definition of $t(j)$ in (3) yields $t(j)=e-j$. Therefore, by (4), $N_j=|K|^j$ $(1\leqslant j<e-1)$. This together with (1) gives

$$N_j=|K|^j,\ 0\leqslant j<e-1;\qquad N_j=|K|^{e-1},\ j\geqslant e-1.$$

By the definition of k_j in Proposition 1,

$$k_j=d(e-j-1),\ 0\leqslant j<e-1;\qquad k_j=0,\ j\geqslant e-1.$$

From this, the identity $l_j=k_{j-1}-2k_j+k_{j+1}$ of Proposition 1 and a simple calculation give

$$l_j=0,\ 1\leqslant j\leqslant e-2;\qquad l_{e-1}=d;\qquad l_j=0,\ j\geqslant e.$$

Thus for p odd and $e\geqslant 3$, $G_0\cong C_{p^{e-1}}\otimes\cdots^{d-1}\otimes C_{p^{e-1}}$. Then, Theorem 18.2 of [7] (see above Note) gives the structure of R^*.

When $p=2$, we have to refine the decomposition of G_0 in (2). The trouble arises because S_1 $(=1+M\backslash M^2)$ fails to be order-homogeneous. By Proposition 3(b), we observe that

$$1+M\backslash M^2\subseteq\{-1_R\}\cup\bigcup_{s=1}^{e-1}-1_R+M^s\backslash M^{s+1}. \tag{5}$$

Further, if $\gamma\in -1+M^s\backslash M^{s+1}$ (with $s\geqslant 2$), we have $\gamma=-1+\alpha 2^s=1+2(-1+2^{s-1}\alpha)$, with $\alpha\in R^*$. Hence $\gamma\in 1+M\backslash M^2$. Thus by letting

$$E_t=(1+M^t\backslash M^{t+1})\cup(-1+M^t\backslash M^{t+1})\qquad(2\leqslant t\leqslant e-1)$$

and

$$E=(1+M\backslash M^2)\cap(-1+M\backslash M^2);$$

we have from (2) and (5) that

$$G_0 = \{1_R, -1_R\} \cup \bigcup_{t=2}^{e-1} E_t \cup E.$$

By Proposition 3, this decomposition is order-homogeneous, with $o(E_t) = 2^{e-t}$ and $o(E) = 2^{e-1}$. It follows that, for $1 \leqslant j < e-1$,

$$N_j = |\{\gamma \in G_0 \mid o(\gamma) \leqslant 2^j\}| = 2 + \sum_{t=e-j}^{e-1} |E_t|$$

(E does not appear because $o(E) = 2^{e-1}$, and $j < e-1$), and then

$$N_j = 2 + 2 \sum_{t=e-j}^{e-1} (|K|^{e-t} - |K|^{e-t-1}) = 2 + 2(|K|^j - 1) = 2|K|^j$$

$(1 \leqslant j < e-1)$.

This and (1) give the complete list of the N_j's:

$$N_0 = 1; \qquad N_j = 2|K|^j,\ 1 \leqslant j < e-1; \qquad N_j = |K|^{e-1},\ j \geqslant e-1.$$

A simple computation, using the definition of k_j in Proposition 1, gives

$$k_0 = d(e-1); \qquad k_j = d(e-j-1) - 1,\ 1 \leqslant j < e-1; \qquad k_j = 0,\ j \geqslant e-1.$$

Then the proof is finished as in the case p odd. ∎

4. The Units of a Chain Ring with Prime char

In this section we obtain the structure of the group of units of a finite chain ring with prime characteristic. As in the previous sections, the key computational tool is Proposition 1.

THEOREM 3. *Let R be a finite commutative chain ring,* char $R = p$ *(p prime). Let K be the residue field of R ($|K| = p^d$) and e the nilpotency index of the maximal ideal M of R. Then*

$$R^* \cong \left(\bigotimes_{j=1}^{\infty} d(\tilde{k}_{j-1} - 2\tilde{k}_j + \tilde{k}_{j+1})\, C_{p^j} \right) \otimes C_{p^d-1},$$

where $\tilde{k}_j = \operatorname{int}_+(e/p^j)$ $(j = 0, 1, \ldots)$.

Furthermore, if $G_0 = 1 + M$ (i.e., the one-group of R), then

$$\operatorname{rk}(G_0) = d(e - \operatorname{int}_+(e/p)).$$

Proof. It is clear that the theorem holds for $e = 1$. Henceforth $e > 1$. We break up G_0 as

$$G_0 = \{1_R\} \cup \bigcup_{t=1}^{e-1} S_t, \qquad \text{with} \quad S_t = 1 + M^t \backslash M^{t+1}. \tag{1}$$

Let π be a generator for M. Clearly, $\gamma \in S_t \Leftrightarrow \gamma = 1 + \alpha\pi^t$ $(\alpha \in R^*)$. As $\operatorname{char} R = p$,

$$\gamma^{p^i} = (1 + \alpha\pi^t)^{p^i} = 1 + \alpha^{p^i}\pi^{tp^i}.$$

Hence

$$\gamma^{p^i} = 1_R \Leftrightarrow \alpha^{p^i}\pi^{tp^i} = 0_R \Leftrightarrow e \leqslant tp^i \qquad \text{(note that } \alpha \in R^*\text{)}.$$

It follows that $o(\gamma) = p^n$, with $n = \min\{i \geqslant 1 \mid e \leqslant tp^i\}$. Thus the classes S_t $(1 \leqslant t \leqslant e-1)$ are order-homogeneous, and

$$o(S_t) = p^{\min\{1 \leqslant i \mid e \leqslant tp^i\}}. \tag{2}$$

It is obvious that as we increase t, $o(S_t)$ decreases. Let $j \geqslant 1$; from (1) and the definition of the N_j's we obtain

$$N_j = |\{\gamma \in G_0 \mid o(\gamma) \leqslant p^j\}| = 1 + \sum_{t=t(j)}^{e-1} |S_t|,$$

with

$$t(j) = \min\{1 \leqslant t \leqslant e-1 \mid o(S_t) \leqslant p^j\}.$$

It follows that

$$N_j = 1 + \sum_{t=t(j)}^{e-1} (|K|^{e-t} - |K|^{e-t-1}) = |K|^{e-t(j)} \quad j \geqslant 1. \tag{3}$$

From (2), $o(S_t) \leqslant p^j \Leftrightarrow \min\{1 \leqslant i \mid e \leqslant tp^i\} \leqslant j \Leftrightarrow e \leqslant tp^j$. Hence

$$\begin{aligned} t(j) = \min\{1 \leqslant t \leqslant e-1 \mid e \leqslant tp^j\} &= \min\{t \geqslant 1 \mid e/p^j \leqslant t\} \\ &= \operatorname{int}_+(e/p^j) \qquad (j \geqslant 1). \end{aligned} \tag{4}$$

Note that $e \leqslant (e-1)\,p^j$ is true for $j \geqslant 1$ and $e > 1$, because $e/(e-1) \leqslant 2 \Leftrightarrow 2 \leqslant e$. This is the reason why the $e-1$ disappeared in (4). Then, from (3) and (4), by observing that $N_0 = 1$ (by the definition of N_j, with $j = 0$), we see that

$$N_j = |K|^{e - \operatorname{int}_+(e/p^j)} \qquad (j = 0, 1, \ldots). \tag{5}$$

From this, direct computation yields $k_j = d(\text{int}_+(e/p^j) - 1)$ $(j = 0, 1, \ldots)$. As it is clear that if we set $\tilde{k}_j = \text{int}_+(e/p^j)$, then $k_{j-1} - 2k_j + k_{j+1} = d(\tilde{k}_{j-1} - 2\tilde{k}_j + \tilde{k}_{j+1})$, Proposition 1 and then Theorem 18.2 of [7] (see the above note) give that R^* has the required structure. Finally, the rank assertion follows readily from noting that $N_1 = p^{\text{rk}(G_0)}$, and (5). ∎

REFERENCES

1. C. W. AYOUB, On diagrams for abelian groups, *J. Number Theory* **2** (1970), 442–458.
2. C. W. AYOUB, On the group of units of certain rings, *J. Number Theory* **4** (1972), 383–403.
3. H. L. CLAASEN, The group of units in $GF(q)[x]/(a(x))$, *Indag. Math.* **39** (1977), 245–265.
4. J. T. CROSS, The Euler ϕ-function in the Gaussian integers, *Amer. Math. Monthly* **90** (1983), 518–528.
5. W. E. CLARK AND D. A. DRAKE, Finite chain rings, *Abh. Math. Sem. Univ. Hamburg* **39** (1973), 147–153.
6. W. E. CLARK AND J. J. LIANG, Enumeration of finite commutative chain rings, *J. Algebra* **27** (1973), 445–453.
7. B. R. MCDONALD, Finite rings with identity, *in* "Pure and Applied Mathematics," Vol. 28, Dekker, New York, 1974.
8. A. A. NEČAEV, Finite rings of principal ideals, *Math. Sb.* No. 3 (1973), 350–366 [In Russian]; *Math. USSR-Sb* **20** (1973), 364–382 [English translation].
9. R. RAGHAVENDRAN, Finite associative rings, *Compositio Math.* **21** (1969), 195–229.
10. A. RANUM, The group of classes of congruent quadratic integers with respect to a composite ideal modulus, *Trans. Amer. Math. Soc.* **11** (1910), 172–198.
11. R. SANDLING, Units in the modular group algebra of a finite abelian p-group, *J. Pure Appl. Algebra* **33** (1984), 337–346.
12. T. H. M. SMITS, On the group of units of $GF(q)[x]/a(x))$. *Indag. Math.* **44** (1982), 355–358.